The Use of Secret Algorithms to Combat Social Fraud in Belgium

Degrave, Elise

Published in:
European review of digital administration & law

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

European Review of Digital Administration & Law - Erdal
2020, Volume 1, Issue 1-2, June-December, p. 167-177
ISBN 978-88-255-3896-0 – DOI 10.4399/978882553896015

*The Use of Secret Algorithms to Combat Social Fraud in Belgium**

Elise Degrave
(Professor at the University of Namur - Director of Research at the Namur Digital Institute NADI/CRIDS)

ABSTRACT Since the nineties, digital administration in Belgium has been built according to an interesting and novel model of data decentralisation within the State. The aim is to protect the privacy of citizens, as soon as the databases are set up. This model therefore embodies the concept of "privacy by design" since then enshrined by the RGPD. Nevertheless, certain tools and practices that have appeared more recently are cause for concern. They seem to destroy the protection of privacy initially organized. In this study, we focus on the OASIS tool, a datawarehouse to which datamatching and datamining techniques are applied to fight against social fraud. The law that seems to frame this tool was adopted very late and is unclear. The information available about OASIS is scarce, even when explicitly requested from the administration. However, this tool makes it possible to collect a large amount of data about many citizens for a very broad purpose, the fight against fraud. There are reasonable grounds for concern that the requirements of legality, transparency and control, which are essential in a democratic state that respects human rights, are not being met in this area. Furthermore, this study highlights the similarities between OASIS and the SYRI tool in the Netherlands. Recently, a decision of the Hague Court recently criticised SYRI by ordering that it should no longer be used, which further reinforces the need to pay close attention to OASIS in Belgium.

1. *Introduction*

In Belgium, the electronic administration, also known as "e-government", is based on a very particular structure: the networking of administrations with the aim of facilitating the exchange of citizens' personal data. This model is guided by two objectives: on the one hand, administrative simplification and, on the other hand, the protection of privacy (par. 1).

This e-government model makes it possible to implement tools and practices to simplify administrative procedures, but also to strengthen the monitoring of citizens' compliance with the rules. In this study, a monitoring tool used to fight social fraud will be of particular interest: OASIS. This tool seems to be hidden by the state. However, it raises many constitutional questions highlighting the delicate balance between administrative efficiency and the protection of fundamental rights (par. 2). This is also what the Dutch judiciary has recently observed with regard to an anti-fraud intelligence tool, SYRI, which has many similarities with OASIS (par. 3).

2. *The Belgian e-government model between administrative simplification and privacy protection*

At the basis of the Belgian e-government and its particular structure, which will be analysed below, there are two strong objectives: administrative simplification and protection of privacy.

2.1. *The objectives of administrative simplification and protection of privacy*

2.1.1. *Administrative simplification*

For a long time, public institutions have worked in a compartmentalised manner, each independently of the other. They collected from citizens the information they needed to carry out their own tasks and did not share it afterwards. It can thus be said that the administration was structured "in silos".

This was a waste of time and money for the administration, which had to contact each person for each piece of information needed, wait for their reply, possibly asking for clarification, but also for the citizen who had to communicate the same information many times to the institutions managing a file about him or her, to carry out administrative procedures that involved identifying the competent administration, travelling, keeping to strict timetables and being patient in the queues.

With the advent of technology, we can see that administrations can now collaborate effectively. Administrative simplification becomes possible. There is now a desire to encourage "synergies between the various departments and levels of government"[1], with the aim of simplifying administrative procedures.

Such collaboration facilitates the work of administrations, which can easily and quickly obtain the data they need to carry out their tasks.

Furthermore, technology makes it possible to

* Article submitted to double-blind peer review.

[1] Commission for the Protection of Privacy (hereinafter "OPC"), Opinion No. 41/2008 of 17 December 2008 on a request for an opinion on the preliminary draft law on the institution and organization of a Federal Service Integrator, No. 5.

reduce the administrative burden on citizens by not having to ask them repeatedly for information they have previously provided and which is already stored in a government database.

From this comes the consecration of a new principle in the administration, the principle of single data collection. This principle consists in asking citizens for information about themselves only once, unlike in the past, when individuals had to repeatedly provide the same data to each administration they were in contact with. In other words, nowadays, as soon as the citizen has provided a certain type of information to one administration, the other administrations cannot ask for it again.

Single data collection and the necessary re-use of data between administrations are not just "good practice". These requirements are contained in legal obligations, in particular a law of 5 May 2014 imposing all federal departments single data collection[2].

2.1.2. *Protection of privacy*

Organising the exchange of personal data between administrations increased the risks that the protection of citizens' privacy would be threatened by abuses in the use of their data. For this reason, a model allowing administrations to work together while minimizing the risks to individual privacy had to be devised.

Should all citizens' data be centralized in a single government database? This was a project that was born in France in the 1970s. The "SAFARI" project consisted in creating a large database called "Automated System for Administrative Files and the Directory of Individuals", in which all the citizens' data necessary for the functioning of the administrations would be grouped together. One of the main concerns of this project was the high risk of data piracy facilitated by the fact that all data would have been available at a single point. Therefore, it was abandoned[3].

In the 1990s, Belgium opted for another model to effectively implement the exchange of information between administrations. This unprecedented model is based on the decentralisation of data among separate administrations, and on the creation of networks of administrations collaborating with each other. Specifically, networks of administrations in which a service integrator ensures the exchange of data between the administrations concerned.

The networked-government model was an early incarnation of the concept of "privacy by design", one of the important principles of the GDPR[4], which calls for privacy to be taken into account at the design stage of the tool. It is exactly this concern for privacy in the architecture of the administration model that led to the choice to organize administration in networks and to abandon the centralized data model.

2.2. *The Belgian model of networked administrations*

How exactly does this model work in practice? First, administrations with something in common (for example, a common work object or membership of the same entity) are grouped together in a set called a "network".

Then, different administrations are assigned the responsibility of collecting, recording and updating specific data. The databases containing this information, each under the responsibility of an administration, are called "authentic data sources". The idea is to ensure that each piece of information relating to the citizen is recorded only once by a single administration of the network, which is then responsible for the reliability of this data.

Finally, a new type of tool is placed at the heart of this network of administrations: the service integrator, also known as an "information exchange platform" or "crossroads bank". In short, the service integrator is a technical infrastructure, placed at the heart of a network of administrations, and which is responsible for ensuring, within this network, the electronic exchange of information from various authentic sources. For example, when an administration needs data that it does not have, it simply contacts the service integrator, which in turn contacts the administration holding the required data and then forwards it to the administration that requested it[5].

In order to facilitate the understanding of this paper, the model of a network of administrations including a service integrator can be schematized as follows.

[2] See Law of 5 May 2014 "guaranteeing the principle of single data collection in the operation of the services and bodies that come under or perform certain tasks for the authority and simplifying and harmonizing electronic and paper forms", accessible here: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2014050506&table_name=loi.

[3] For more information on this subject, see https://www.senat.fr/evenement/archives/D45/context.html.

[4] Art. 26 GDPR.

[5] For further developments on e-government and the networked government model, see D. De Bot, *Privacybeschermingbij e-government in België. Eenkritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingenen de elektronische identiteitskaartals belangrijkste juridischebouwstenen*, Brugge, VandenBroele, 2005, 1-13; E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Brussels, Larcier, 2014, in particular 172 ff.

Diagram illustrating a network of administrations made up of a service integrator to which several administrations are linked, some of which hold an authentic source of data.

In concrete terms, there are several networks of administrations in Belgium, concerning health, social security, tax, vehicles, etc. In the following lines, we focus on the social security network whose service integrator is called the "Crossroads Bank for Social Security".

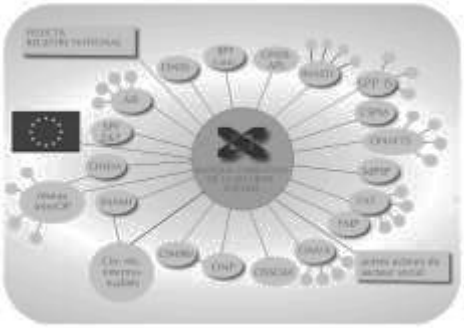

Diagram of the social security network, with the Crossroads Bank for Social Security at its heart.

3. *OASIS to combat social fraud*

This e-government model makes possible new operations within the public sector based on the re-use of citizens' personal data.

The administration can thus automatically grant certain benefits to those entitled to them[6].

It can also exercise more control over citizens. The fight against social fraud is a very telling example of this phenomenon, made possible by the use of a "data warehouse" called "OASIS" to which the data matching and data mining techniques are applied.

3.1. *Data warehouse, data matching and data mining*

To reinforce the fight against social law fraud, the Belgian administration has created a "data warehouse" called "OASIS", namely "Organisation Anti-fraude des Services d'Inspection Sociale". This is a large database containing a large amount of data on companies and individuals, so that social fraud can be effectively identified.

This system has been operational since 2005[7].

After analysing the content of the OASIS "data warehouse", social profiling will now be studied.

3.1.1. *The OASIS "data warehouse"*

As a "data warehouse", OASIS is a special database, which is characterised mainly by the fact that it contains a considerable amount of information, organised according to a certain logic, which makes it possible to carry out complex searches on the basis of that information.

OASIS contains mainly data on employers and workers of certain sectors of activity, such as the construction sector and the hotel and catering industry. These data come from a number of different databases held by the government. These include tax data, social security data, pension data, ... Recently, OASIS also contains data provided by energy suppliers (gas, water and electricity) about their customers[8].

OASIS "Datawarehouse" and some databases that provide data to OASIS.

3.1.2. *Data mining and data matching*

Before the use of OASIS, people suspected of social fraud were identified by social inspectors based on their knowledge of social fraud. They described the type of fraudster sought to the computer specialists in order to establish certain computer links between the files held by the administrations concerned.

The weakness of this system was linked to the fact that, at one point, the social inspectors had provided all their knowledge without, however, all the frauds having been discovered. Their work also depended on the complaints of workers, who over time, due to legislative changes, were less and less numerous.

Today, these human limits are being surpassed thanks to the powerful calculations carried out by OASIS, which allow more potential fraudsters to be identified.

[6] For more information on this topic, see E. Degrave, *L'e-gouvernementet la protection de la vie privée. Légalité, transparence et contrôle*, 33 et seq.

[7] Analytic Report of the Social Affairs Committee, *Doc. Parl.*, sess. 2004-2005, COM 541, 19.

[8] See below.

OASIS is used to perform profiling operations, i.e., subjecting an individual's data to a calculation software that is capable of performing statistical comparisons and correlations. Depending on the result of these calculations, the individual is attached to a predetermined category of the population, which presents specific characteristics justifying a particular attitude, such as, in the case of OASIS, an inspection for suspected social fraudsters[9].

In concrete terms, this profiling operation is carried out by means of data matching and data mining operations.

Data matching consists in comparing data. A number of alarms are applied to the data recorded in OASIS. These alarms are fraud detection algorithms relating some specific data to each other.

Once the data matching operation is completed, the *data mining* operation is performed. This operation is at the heart of the concept of profiling, which the Council of Europe defines as "an automated data processing technique that consists in applying a 'profile' - that is, a set of data that characterises a category of individuals - to a natural person, in particular in order to take decisions about him or her or to analyse or predict his or her personal preferences, behaviour and attitudes"[10].

Let us take an example which, for the sake of clarity of this paper, oversimplifies this very complex technique. John is 30 years old and is a researcher at the University. His tax data show that he earns an average salary. Statistically, he should be in the category of citizens with a small car and a modest home. However, the vehicle data shows that John drives a new Ferrari. The National Register indicates that his home is located in a wealthy city, and tax data shows that the property tax on his home is high. Is John guilty of social or tax fraud? In any case, suspicion is the order of the day. John falls into the category of presumed tax and social fraudsters and a tax and/or social audit will be encouraged.

In other words, by performing data mining, one connects an individual to a particular person's profile, based on the data that has been analysed about him or her. In this case, the fact that an alarm is triggered at the time of the data cross-referencing results in the individual being linked to the profile of the alleged fraudster for the type of fraud targeted by the alarm. Therefore, the data matching and data mining operations make it possible to identify individuals who are potential fraudsters.

Once identified, the identity of the natural or legal person is communicated to the social inspection services. The latter will then carry out a control on the persons concerned.

OASIS is therefore an administrative decision support tool, but it does not take the decision to establish and punish fraud by itself. It is therefore not possible, at present, to challenge the decisions taken by OASIS. Nonetheless, in our opinion, OASIS takes important decisions in the functioning of the administration. For example, classifying a person as a "potential fraudster" is a decision taken by an algorithm, which then strongly influences the administration's decision to identify and, if necessary, punish a fraud. This set of elements raises questions and requires the OASIS tool to be precisely framed[11].

3.2. *Applications*

As has been said, OASIS is used to fight social legislation fraud. There are several applications of this tool[12]. Two of them are identified in this study.

OASIS is used to combat *fraudulent labour providers and bankruptcies*[13]. These are companies that hire many workers, declare each worker but do not pay the social security charges relating to them to the National Social Security Office (NSSO). By the time the NSSO realises this and decides to carry out an inspection, the workers concerned are moved - often in large numbers - to another company, which repeats the same type of fraud. In OASIS, a first alarm makes it possible to detect the mass arrival of these workers who will be declared but for whom the employer will not pay social security contributions, and a second alarm makes it possible to show that as of the arrival of these workers, debts towards the NSSO have arisen.

In addition, since 2016, OASIS has been used to fight against the *domicile fraud*, also called

[9] M. Hildebrandt, *Who is Profiling Who? Invisible Visibility*, in *Reinventing Data Protection?*, S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, and S. Nouwt (eds.), *Dordrecht*, Springer, 2009, 241; V. Papakonstantinou, *A Data Protection Approach to Data Matching Operations Among Public Bodies*, in *International Journal of Law and Information Technology*, vol. 9, n. 1,2001, 62-63; J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever and A. Rouvroy (eds.), *L'application de la Convention 108 au mécanisme de profilage. Eléments de réflexion destinés au travail futur du Comité consultatif (T-Pd)*, Strasbourg, publication of the *Comité consultatif de la Convention pour la protection des personnes a l'egard du traitement automatisedes donnees a caractere personnel*, 2008, 5.

[10] Recommendation CM/Rec (2010)13 of the Committee of Ministers of the Council of Europe to Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, available at www.coe.int.

[11] See below.

[12] These applications are explained here: https://www.ksz-bcss.fgov.be/fr/services-et-support/services/lutte-contre-la-fraude.

[13] E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, 44.

fictitious domicile[14]. In this situation, one person declares a family situation or a domicile that does not correspond to reality in order to receive more social assistance than he or she is entitled to. It is therefore mainly the poorest people who are targeted by this use of OASIS. For example, a man receives unemployment benefit. He lives alone in an apartment, which enables him to receive a higher unemployment benefit than if he declared living as a couple. In reality, he lives with his partner. This is a fictitious domicile. To fight against this type of fraud, the administration relies on data sent by energy suppliers (gas, electricity, water). They are legally obliged to send the data of customers, whose private consumption deviates by at least 80 per cent up or down from an average consumption depending on the officially communicated household composition, to the Crossroads Bank for Social Security, which manages OASIS[15]. Then, the data matching operation begins: among these clients, the beneficiaries of social benefits are identified on the basis of their other data held by the administration. The data mining operation follows: the fact of being identified as a beneficiary of a social allowance, with an abnormally low or high energy consumption, leads to linking the person to the profile of the alleged fraudster and triggers an alarm indicating that the person must be monitored by a social inspector.

3.3. *Poor law and hidden information*

3.3.1. *A very late and poor quality legal framework*

OASIS has been operational since 2004. Although it constitutes a significant interference in the private life of citizens, since it processes a large amount of data relating to many of them, it was not regulated by any law between 2004 and 2018. In a particularly dense law of 5 September 2018, the Belgian legislator discreetly slipped a provision[16] that seems to be intended to frame OASIS, without explicitly mentioning it.

This provision is formulated in an unclear and very broad manner. In short, the law authorises the collection of all personal data for fraud prevention purposes.

Indeed, it can be inferred from the law that a large number of public institutions (e.g. all social security institutions and social inspection services) can collect a lot of data (i.e. "all data necessary for the purposes of the enforcement of legislation concerning labour and social security law") and make extensive use of them ("collect, process and aggregate them in a "data warehouse" enabling them to carry out data mining and data matching operations, including profiling within the meaning of Article 4, 4) of the General Data Protection Regulation). The purposes mentioned by the text are also very numerous ("the prevention, detection, investigation, prosecution and punishment of offences against social regulations (...), and the collection and recovery of the amounts falling within their respective powers").

3.3.2. *Access to information is almost impossible*

In addition to the fact that the law is of poor quality and does not provide the necessary information on how OASIS works in practice, when trying to understand how OASIS works in practice, it is particularly burdensome to access public information about this tool. In short, information about OASIS seems to be hidden.

Initially, while studying the decisions of the Belgian data protection authority, by chance we found some trace of the name "OASIS" for the first time. We then wanted to know more. The task was so tedious that we felt like an investigative journalist. In exercising our right to access administrative documents with a public authority involved in setting up OASIS, we were unable to gain access to official documents on this subject, on the grounds that the document could be a "source of misunderstanding"[17] within the meaning of the law on the publicity of the administration. After having appealed to the Commission for Access to Administrative Documents, the Commission replied that the authority addressed was not an administrative one and that the requirements of transparency did not therefore apply[18].

When we spoke to officials in the administrations, we received several replies

[14] See the Law of 13 May 2016 amending the programme Law (I) of 29 March 2012 concerning the control of the abuse of fictitious addresses by recipients of social benefits, with a view to introducing the systematic transmission of certain consumption data from distribution companies and distribution network operators to the BCSS improving data mining and data matching in the fight against social fraud http://www.ejustice.just.fgov.be/loi/loi.htm.

[15] Article 2 of the aforementioned Law of 13 May 2016.

[16] Article 12 of the Law of 5 September 2018 establishing the Information Security Committee and amending various laws concerning the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, accessible here: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.-pl?language=fr&la=F&cn=2018090501&table_name=loi.

[17] Letter from the President of the *Sectoral Social Security Committee* dated 11 August 2011.

[18] Committee on Access to and Re-use of Administrative Documents, *Opinion No. 2011-309* of 10 October 2011, on the refusal to grant access to documents which have been used by the *Sectoral Committee on Social Security and Health* to take a decision, available here: ht tps://www.ibz.rrn.fgov.be/fileadmin/user_upload/fr/com/publicite/avis/2011/AVIS-2011-309.pdf.

explaining that either one department was not competent, or that they did not know the matter, or that the file was transferred to this or that department. We had to rely on the cooperation of two administrative officers who agreed to give us information in confidence to understand what it was all about.

Having made new access requests since the publication of the law of 5 September 2018, we cannot help but notice that the situation has not changed. We are either directed to information that is not related to OASIS[19], or sent from one administration to another.

In the end, to date, we have not been able to access an official document clearly explaining this tool. All we have found as public information is a web page, hosted on the website of the Crossroads Bank for Social Security, which explains in a very enthusiastic and synthetic way the effectiveness of OASIS in the fight against fraud. However, we still have no explanation of the essential elements on which OASIS is based, such as an exhaustive list of the data aggregated in the "data warehouse", a clear list of the purposes pursued, the algorithms used, an explanation of the types of alarm, etc.

3.4. *Violation of several fundamental rights*

The fact that the legislation surrounding OASIS is of poor quality and that accessing information about this tool is very difficult if not impossible, constitutes a violation of the protection of citizens' privacy and also threatens other fundamental rights.

3.4.1. *A violation of the fundamental right to privacy*

During the preparatory works for the law of 5 September 2018, the Data Protection Authority[20] was very critical. Among other things, it argued that the law was not sufficiently clear, in particular with regard to the purposes, formulated in a "broad and comprehensive" manner that "offers (...) very few points of reference for the subject whose data are to be found in the "data warehouse(s)". Neither Article 8 of the European Convention on Human Rights (hereafter ECHR), nor Article 22 of the Constitution, nor the GDPR, in particular Articles 6.3 and 22, authorise such a 'blank cheque'[21].

The legislative section of the Council of State had also issued a very critical opinion on this law, stressing in particular that "the creation of a "data warehouse" processing a large number of data and concerning a large part, if not all, of the citizens and possibly using profiling techniques cannot be considered as insignificant", which is why the legislator must precisely determine the essential elements of these data processing operations[22].

The text had then been slightly modified, notably by integrating a summary definition of the terms "data matching" and "data mining", but without making any real improvements to the text.

Today, the situation remains worrying. Among other criticisms, OASIS is a clear intrusion into the privacy of citizens. It gathers a large amount of citizens' personal data from multiple government databases.

This information was initially collected by the administrations for the performance of specific legal tasks, such as the payment of allowances to beneficiaries, and not for the purpose of profiling them. Therefore, OASIS re-uses data for a different control purpose from the one pursued when the information was collected, without informing the data subjects.

Furthermore, data mining is a powerful data processing operation which inherently presents dangers, especially when a general profile is erroneously attributed to a particular person.

Moreover, OASIS is, of course, a tool supporting the administrative decision-making which does not take the decision itself to establish and sanction a fraud. Nevertheless, attributing the qualification of "potential fraudster" to a person is, in our opinion, a decision taken by an algorithm, which then strongly influences the administration's decision to detect and, if necessary, sanction a fraud. This set of elements raises questions with respect to the GDPR[23], which prohibits fully automated decision making.

In view of these flaws and the vagueness of the legal provision that is supposed to govern OASIS, the current situation is, in our view, contrary to the GDPR but also to the Belgian Constitution. Indeed, in Belgium, the protection of privacy is a fundamental right enshrined in Article 22 of the Constitution. This right is also enshrined in Article 8 of the European Convention on Human Rights. It follows from the case-law of the European Court of Human Rights[24], the Constitutional Court and the

[19] For example, on 7th July 2020, the Crossroads Bank for Social Security referred us to this website: https://www.ksz-bcss.fgov.be/fr/dwh/homepage/index.html.

[20] Formerly known as the "*Commission de la protection de la vie privée*".

[21] CPVP, *Opinion No. 34/2018*, No. 29 available here: https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_34_2018_0.pdf

[22] Legislative section of the Council of State, Opinion No. 63.202/2 of 26th April 2018, Doc. Parl, Ch. repr., session 2017-2018, Doc 54 3185/001, p. 138 accessible here: https://www.lachambre.be/doc/FLWB/pdf/54/3185/54K3185001.pdf.

[23] Art. 22 GDPR. See below.

[24] See Coureur D.H., Rotaru v. Romania judgment, 4 May 2000, Req. 28341/95, § 57.

Council of State[25] that the legislator is obliged to determine the "essential elements" of data processing in a clear and precise manner. In other words, the law must be irreproachable in terms of its content.

In this case, this means that the law governing OASIS must be sufficiently clear, so that the citizen can know, by reading the law, what is going to happen to the data he or she entrusts to the state. The law must therefore set out precisely the essential elements of the interference, i.e., the guidelines governing the use of OASIS (purposes of the data processing implemented, data used, recipients of the data, obligation to inform subjects of this use of their data, control of the tool, etc.). These elements are not currently found in the law[26].

Article 22 of the Constitution also requires the adoption of a law in the formal sense of the term, in order to interfere in the private life of citizens. The need for a formal law is meant to stimulate the democratic debate and to reflect on how the delicate balance between administrative efficiency and privacy can be achieved in the use of OASIS. However, in the case of OASIS, this debate has not taken place. The legal provision that was supposed to govern OASIS was included in a very long "catch-all" law, drafted just before the summer, in very technical language, so that the issues behind it did not receive sufficient attention from MPs and were not debated. The result is a technical provision, designed by technicians, aimed more at administrative efficiency than at respecting the fundamental rights of citizens. Therefore, OASIS is a tool that to this day remains largely unknown to the public but also to the leaders of our country.

Finally, we must unfortunately note that the protection of privacy, cleverly put in place by the networked administration model[27], is destroyed by this data warehouse which gathers in a single point initially decentralized data, and allows all possible reuses to achieve the very broad purpose of the fight against fraud.

3.4.2. *Secret algorithms maybe discriminatory*

There's more. In addition to the violation of privacy and personal data protection, the OASIS tool also raises questions with regard to other fundamental rights. These include equality and discrimination. Given the limited public information available about OASIS, combined with the fact that it is currently not possible to access administrative documents that would allow one to understand how OASIS works, the algorithms used in the data matching and data mining remain secret and therefore impossible to control.

However, it would be very useful to be able to analyse these algorithms to check, for example, that they are not affected by algorithmic, racist, sexist or "anti-poor" biases. Indeed, we know that algorithms are not neutral. They are the result of decisions made by algorithm developers who, consciously or unconsciously, make choices[28]. However, these human choices can indirectly orient the algorithm, and therefore the decision taken on the basis of the algorithm, in favour or against certain categories of people. This is called "algorithmic bias": the algorithm is not neutral and therefore leads to an oriented decision. This biased decision may, for example, be more in favour of white-skinned people than black-skinned people, richer than poor, men than women. There is therefore a risk that using secret algorithms to make public decisions may lead to "automating inequalities"[29] at the societal level.

In this case, nothing is known about OASIS algorithms. It cannot be ruled out that the profiling implemented in the fight against social fraud primarily targets certain populations and neighbourhoods, thus leading to serious discrimination. This situation is very worrying and unacceptable in a state governed by the rule of law.

3.4.3. *The power of decision delegated to algorithms*

A computer tool alone cannot make an administrative decision. Indeed, Article 33 of the Belgian Constitution states "All powers emanate from the Nation. They shall be exercised in the manner laid down by the Constitution".

From this follows the principle of the unavailability of powers, according to which the administrative authority must itself carry out the tasks legally assigned to it, effectively exercising its discretionary power.

Giving decision-making power to algorithms would be contrary to the principle of unavailability of powers enshrined in Article 33 of the Constitution. It would be similar to delegating competence to a computer tool.

For example, the Council of State has already been seized of several appeals concerning the use

[25] See. E. Degrave, *L'e-gouvernementet la protection de la vie privée. Légalité, transparence et contrôle*, 103 and references cited.

[26] In the same sense, see. Commission de la protection de la vie privée, Opinion No. 34/2018 of 11 April 2018, No. 26 ff. https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_34_2018_0.pdf.

[27] See above.

[28] About that, see C. O'Neill, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, USA, Crown Books, 2016.

[29] V. Eubanks, *Automating inequality. How high-tech tools profile, police and punish the poor*, New York, St Martin's Press, 2018.

of a computer tool in the context of the award of a public contract. The administrative authority is accused of not being able to explain its choice, which is too largely dictated by the calculations made by the computer[30].

In the present case, the administration could not therefore let OASIS decide on a sanction related to the person suspected of fraud through its algorithms. An algorithm does not understand reality and therefore could not itself adopt a decision and give reasons for that decision.

For this reason, the identification of a possible fraud by OASIS must be followed by an on-site inspection and it is during this inspection that the reality of the fraud will be verified. In the event of fraud, the penalty will be imposed by the administration on the basis of the grounds identified by the inspectors.

However, between the identification of the possible fraudster and the on-site inspection, there is, in our view, an intermediate administrative decision that is adopted: the decision to carry out an on-site check. This decision is based largely on a tool that the social inspectors themselves do not understand since they do not understand how OASIS identifies potential fraudsters. Therefore, one may wonder whether the administrative decision to sanction a fraud is, in part, the result of a delegation of competence to an algorithm, which would be unconstitutional.

This issue, which has not yet been resolved to date, is related to Article 22 of the GDPR, which prohibits fully automated decisions. The identification of a potential fraudster is an essential part of the process that will lead to the sanctioning of an individual. Without this identification, there can be no control and without control, there can be no sanction. At present, this identification is carried out in a fully automated manner, by OASIS, and in a completely opaque manner given the lack of accessible information about this tool. Should not the importance of this automated and opaque operation in the process of sanctioning a fraud lead to the recognition that the decision to sanction a fraud is contrary to Article 22 of the GDPR? This is a question that is still pending at this stage of our research.

4. *Towards a reconsideration of OASIS at the start of the SYRI case?*

Recently, a very interesting case has arisen in the Netherlands concerning a tool that has many similarities with OASIS.

4.1. *The SYRI tool*

The SYRI tool, namely System of Risk Indicator, is under the responsibility of the Dutch Ministry of Social Affairs and Employment. Just like OASIS, it is an automated system for monitoring social fraud. A data matching operation gathers 17 categories of data (tax data, pension data, social assistance data, etc.). These are then subjected to the data mining technique to identify citizens who are suspected of fraud. Each individual or legal entity suspected of fraud is given a score that corresponds to a risk notification.

Like OASIS, this system was first created and used outside any legal framework[31]. Initially, the Dutch press caused a scandal by revealing that Bulgarian gangs had been committing social fraud for many years. When they arrived in the Netherlands, they registered as residents, opened a bank account and applied for social assistance. They then returned to Bulgaria, continuing to receive social benefits for years. SYRI was created to make the fight against this type of fraud more effective[32]. In 2014, the legislator gave the tool a legal basis. SYRI is governed by articles 64 and 65 of the law *Structuur uitvoeringsorganisatie werk en inkomen* and chapter 5, letter a), of its implementing decree.

4.1.1. *Reactions and legal action*

As soon as it was set up, SYRI aroused a lot of reactions. The Council of State and the Data Protection Authority highlight the fact that SYRI violates the protection of citizens' privacy, in particular because the purpose of the tool is too broad, the principle of data minimization is not respected, and data are reused for purposes incompatible with those of their initial collection[33]. In addition, NGOs point out the risk that the algorithms used may be subject to discriminatory bias, based on a survey showing that SYRI is used mainly in poor neighbourhoods or neighbourhoods with a high percentage of migrants[34].

These NGOs, as well as experts and journalists, then filed a lawsuit before the District Court of The Hague[35]. The plaintiffs based their

[30] See C.E., 16th September 2004, *Computer Sciences*, n. 134.986; C.E., 7 March 2006, *SA Construction industrielles de la méditerranée et alii*, n. 155.931; C.E., 8th June 2006, *NV Eurosense Belfotop*, n. 159.782; C.E., 27th December 2006, *N.V. Bioterra et alii*, n. 166.318.

[31] See the intervention in this case by Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights, "*Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388)*" available here: https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf.

[32] Society for Comparative Legislation, Netherlands Report, 9, available here: https://www.legiscompare.fr/web/Activites-de-la-section-921.

[33] *Ibidem*, 11 and 12.

[34] *Ibidem*,14.

[35] The applicants' submissions are available here:

action on two grounds. On the one hand, SYRI violates the legal regime for the protection of privacy and, in particular, Article 8 §2 of the European Convention on Human Rights, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, Article 17 of the United Nations Covenant on Civil and Political Rights and Articles 5, 6, 13, 14, 22 and/or 28 of the GDPR[36]. On the other hand, SYRI violates the right to an effective remedy and the right to a fair trial as guaranteed by Articles 6 and 13 of the Convention, Article 47 of the Charter of Fundamental Rights of the European Union[37].

4.1.2. *The judgment of the District Court of The Hague*

The Court delivered its judgment on 5 February 2020[38]. In this judgment, the court measures SYRI mainly against Article 8 §2 of the European Convention on Human Rights.

First of all, the court recognises that SYRI pursues a *legitimate objective*, namely the economic well-being of the country. "Social security is one of the pillars of the Dutch society and contributes significantly to the prosperity of the Netherlands" and "new technologies - including digital options for linking files and analysing data using algorithms - (...) must be used to prevent and combat fraud"[39].

The Court then points out that SYRI constitutes an *organised interference with the privacy of citizens*, which is extensive and serious, particularly in view of the "very large category of data processed", the lack of transparency as to the model and risk indicators used, and the lack of information of the data subjects[40]. The United Nations Special Rapporteur on Human Rights and Extreme Poverty, Philip Aston, explained it very well in his third intervention in this case. He explained that "the essence of the right to privacy is at stake here. Entire neighbourhoods are deemed suspicious and are subject to special scrutiny, which is the digital equivalent of fraud inspectors knocking on every door in a certain area and examining the files of every individual in an attempt to identify cases of fraud (…). In the real world, there would never be enough fraud inspectors to undertake such an exercise and the general public would quickly resist and protest against such invasions of their privacy. The fact that SYRI operates in the digital realm and not in the real world is just a little solace, however, for those affected by it. The psychological and other effects of a physical raid on a neighbourhood by fraud inspectors is relatively easy to imagine, but a digital raid of such magnitude leaves equally problematic traces. The fact that SYRI operates in relative silence and is de facto invisible to the naked eye may in fact increase the discomfort and harm suffered by people living in these neighbourhoods"[41].

According to the Court, this interference is *disproportionate* to the objective pursued by SYRI. Indeed, "the SYRI legislation (...) does not respect the *fair balance* required for a justified interference within the meaning of Article 8(2) of the ECHR"[42].

The Court relies on the fact that the law does not provide sufficient guarantees for the citizen by failing to respect the fundamental principles of privacy and personal data protection, namely transparency, purpose limitation and data minimisation[43]. Among other things, the fact that "the SYRI legislation does not provide information on the functioning of the risk model, for example, on the type of algorithms used in the risk model"[44] makes it "difficult to see how a data subject can defend himself against the fact that a risk report has been drawn up for him"[45].

The tribunal also added that this lack of transparency is problematic because, while risk analysis is useful, it can lead to "discriminatory (unintended) effects"[46]. However, under the current SYRI legislation, "it is not possible to assess whether this risk has been sufficiently mitigated due to a lack of verifiable knowledge about risk indicators and the (operation of the) risk model"[47].

Consequently, the court decided that Article 65 of the law *Structuur uitvoeringsorganisatie werk en inkomen (SUWI)* and chapter 5, letter a), of its implementing decree have no binding effect on the claimants.

The effect of this decision is the immediate cessation of the use of SYRI.

4.1.3. *Will the "SYRI case" inspire an "OASIS case"?*

The decision of the District Court of The Hague states, very usefully, that even if the

https://pilpnjcm.nl/wp-content/uploads/2015/12/Pleitnotities-NJCM-c.s.-inzake-SyRI.pdf.

[36] See the above conclusions, 5 ff.

[37] See the above conclusions, 11 et seq.

[38] The ruling is available here: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865.

[39] The above-mentioned ruling, n. 6.3 and 6.4.

[40] *Ibidem*, n. 6.65.

[41] P. Alston, *Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388)*, n. 29, available here: https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf.

[42] *Ibidem*, n. 6.83.

[43] *Ibidem*, n. 6.86.

[44] *Ibidem*, n. 6.89.

[45] *Ibidem*, n. 6.90.

[46] *Ibidem*, n. 6.91.

[47] *Ibidem*, n. 6.94.

technological tools have a legitimate purpose, they must respect the fundamental rights of citizens. In particular, even if powerful anti-fraud systems pursue a legitimate interest in a State governed by the rule of law, they must respect the rules of privacy and personal data protection so as not to upset the subtle balance between administrative efficiency and protection of citizens' freedoms.

The fundamental principles of data protection, enshrined in the GDPR, must therefore be respected. In particular, every citizen should be able to know, and understand, what will happen to the data he or she entrusts to the State, thanks to a clear knowledge of the data used and the purposes pursued.

However, and this is a remarkable point of this judgment, the court is not content with simply ensuring the protection of personal data as defined by the GDPR. This decision is also a step forward for the transparency of the algorithms. Indeed, this decision clearly underlines that the secret nature of the risk models, risk indicators and types of algorithms used in the fight against fraud violates the fundamental requirement of transparency imposed by Article 8(2) of the ECHR, even though this information does not, in itself, constitute personal data. This link is very interesting at a time when it is regrettable that the GDPR has limited the notion of "data" to "personal data", thus preventing the protection of individuals from the impact of algorithms used in State decisions. The court also highlights the need for the legislator who sets up such computer systems to ensure that algorithmic biases, and thus the risks of discrimination, are eradicated or at least minimized. This is a first step towards the possibility of challenging, in court, the opacity of algorithms. It is to be hoped that, in the near future, it will be possible to challenge directly the algorithms used by public authorities, without having to appeal the administrative decisions resulting from them[48].

The similarities between OASIS and SYRI are obvious. It is to be hoped that the lessons learned from this remarkable decision will inspire a review of the OASIS tool in Belgium.

5. *Conclusions*

Whether it is to lighten the administrative burden, to combat fraud or to grant allowances to those who are entitled to them, digital tools must be used to achieve administrative efficiency. However, the efficiency of public authorities cannot ignore fundamental rights, otherwise confidence in the State in general, and digital administration in particular, will be undermined.

In Belgium, the e-government model was developed from the outset, taking into account both the need for efficiency and the protection of citizens' freedoms. This model gives concrete expression to the idea of "privacy by design" well before its affirmation by the GDPR.

Unfortunately, since then, new tools have appeared within the administration that do not take sufficient account of this delicate balance. This is the case, for example, with the OASIS tool. The privacy protection made possible by the decentralisation of data seems to be undermined by the fact that this tool uses a lot of data to fight fraud, aggregates it in a data warehouse, processes it for unclear purposes. The law being unclear, and the scarcity or non-existence of public IT on this subject makes OASIS an algorithmic black box. This black box is, for the moment, uncontrollable. Thus, are the algorithms used by OASIS not affected by bias, which would lead the administration to target poor categories of the population as a priority?

Such uncertainty surrounding the use of citizens' personal data is not acceptable in a state governed by the rule of law, as it violates Article 8 §2 of the European Convention on Human Rights and, in Belgium, Article 22 of the Constitution.

This situation risks gradually undermining the citizen's confidence in the State. However, this confidence is essential in terms of digital administration. Without it, citizens will no longer agree to entrust their data to the State and will no longer support new digital practices in the future. The European Court of Human Rights has already affirmed this, stating that "any state which claims a pioneering role in the development of new technologies bears a particular responsibility to strike the right balance in this area", by carefully weighing "the advantages which may result from the extensive use of these technologies against the essential interests of the protection of privacy"[49]. In the same sense, in Belgium, the Council of State has stressed the "serious breach of public confidence" with regard to illegal data processing carried out within the administration.

Ultimately, the reactions provoked by the use of technology by the State are a reminder that progress in the digital world can only be made if the relationship between the State and citizens is conceived as a partnership based on mutual trust. This trust cannot be imposed by binding legislation. It must be inspired by respect, in this

[48] In this sense, G. Lewkovitch, *Les outils d'intelligence artificielle contre les droits de l'homme: l'affaire NJCM C.S./De staat der Nederlanden*, accessible here: https://www.incubateurbxl.eu/fr/les-outils-dintelligence-artificielle-contre-les-droits-de-lhomme-laffaire-njcm-c-s-de-staat-der-nederlanden/.

[49] ECHR, *S. and Marper v. the United Kingdom*, 4th December 2018, Applications N. 30562/04 and 30566/04, § 112. The judgment can be accessed here: http://hudoc.echr.coe.int/fre?i=001-90052

new context, for the founding pillars of the rule of law.

Thus, digital technology challenges the State to respect legality, transparency and control.

With regard to *legality*, even if the digital tools are technical, their implementation cannot do without a democratic debate on the necessary balance between administrative efficiency and the protection of citizens' rights. It is not up to the administration to find this balance, but to the legislator to define it after a thorough democratic debate in order to define solutions that are in line with the values of society as a whole. Without this legality, it is also the *legitimacy* of state action that will be affected.

The principle of *transparency* requires that the digital tools used by the State should be known to the public, as the SYRI case has again reminded us. We cannot win the confidence of citizens by keeping them in ignorance. These tools must be known, but they must also be understandable. Transparency in the digital world requires the State to make a special educational effort to enable everyone to understand what will happen to the data they entrust to the State.

Finally, these digital tools must be able to be *controlled*, not only by the judiciary but also by anyone interested in them. This is particularly important at a time when more and more algorithms are being used, which may contain discriminatory biases.